Software Requirements Specification

For

Global Alert Resolution NETwork (GARNET)

Version 2.0

Prepared by:

NASA Goddard Space Flight Center
Advanced Architectures and Automation Branch, Code 588
Julie Breed, Code 558 Branch Head
Stephanie Nickens, Code 588 GARNET ATR
Corinne Irwin, Code 585 GARNET System Architect

December 21, 2004

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Intended Audience and Reading Suggestions 1
1.3 Project Vision 1
1.4 Project Scope 2
1.5 References 2
2 Overall Description 2
2.1 Product Features 2
2.2 User Classes and Characteristics 3
3 System Functional Requirements 4
3.1 Alert Definition 4
3.2 Login 6
3.3 User Profile Management 7
3.4 Alert Creation 9
3.5 Alert Notifications 10
3.6 Alert Searches 13
3.7 GARNET Desktop Client 14
3.8 Administrative 14
3.9 Documentation and Help 17
3.10 Logging 18
4 System Nonfunctional Requirements 19
4.1 Performance Requirements 19
4.2 Security Requirements 19
4.3 Fault Tolerance 21
4.4 Software Quality Attributes 22
5 Other Requirements 22
5.1 System Constraints 22

Revision History

Name	Date	Reason For Changes	Version
Original	1/27/2003	Initial Release	1.0
	2/6/2003	Integrated feedback from Stephanie Nickens	1.1
	2/12/03	Integrated feedback from Julie Breed	1.2
	12/21/2004	Update for Production version of GARNET	2.0

1 Introduction

1.1 Purpose

The purpose of this document is to describe the functional and system requirements for the Global Alert Resolution Network (GARNET). The requirements specified in this document encompass the functionality for the first production release of GARNET.

The document contains two levels of requirements. The first level of requirements outlines broad user and system functionality that is necessary to achieve the overall goals of GARNET. The second level of requirements details the specific functionality that will be included in GARNET 2.0. GARNET 2.0 encompasses the system functionality necessary for initial rollout to the Goddard Space Flight Center's (GSFC's) Greenbelt Facility. In the case that a customer wishes to alter and/or extend GARNET 2.0, an additional requirements document should be produced outlining the altered and/or new functionality.

1.2 Intended Audience and Reading Suggestions

Each section of requirements in this document is separated into two sections, high level and GARNET 2.0. The intended audience for the high level requirements includes the following:

- Project Managers
- Marketing Staff
- System Analysts
- Developers
- Testers

The second level of requirements, GARNET 2.0, provides detailed system requirements and is intended for the following audiences:

- Project Managers
- Developers
- Testers
- User-manual authors

Those not interested in the detailed requirements may skip the GARNET 2.0 sections of the document.

1.3 Project Vision

The ultimate goal of GARNET is to deliver time-critical information to all affected people in the case of an emergency such as a national security concern, an intrusion, or severe weather event.

The following is a list of high-level goals of the GARENT alerting system.

- Rapidly distribute alerts with detailed information and instructions
- ***Broadly*** distribute alerts to users regardless of physical location, available technologies, and personal physical disabilities

- Target the distribution of alerts to pertinent individuals, preventing users from receiving irrelevant alerts.
- Provide high reliability
- Function at low cost in terms of both funding and system resources

1.4 Project Scope

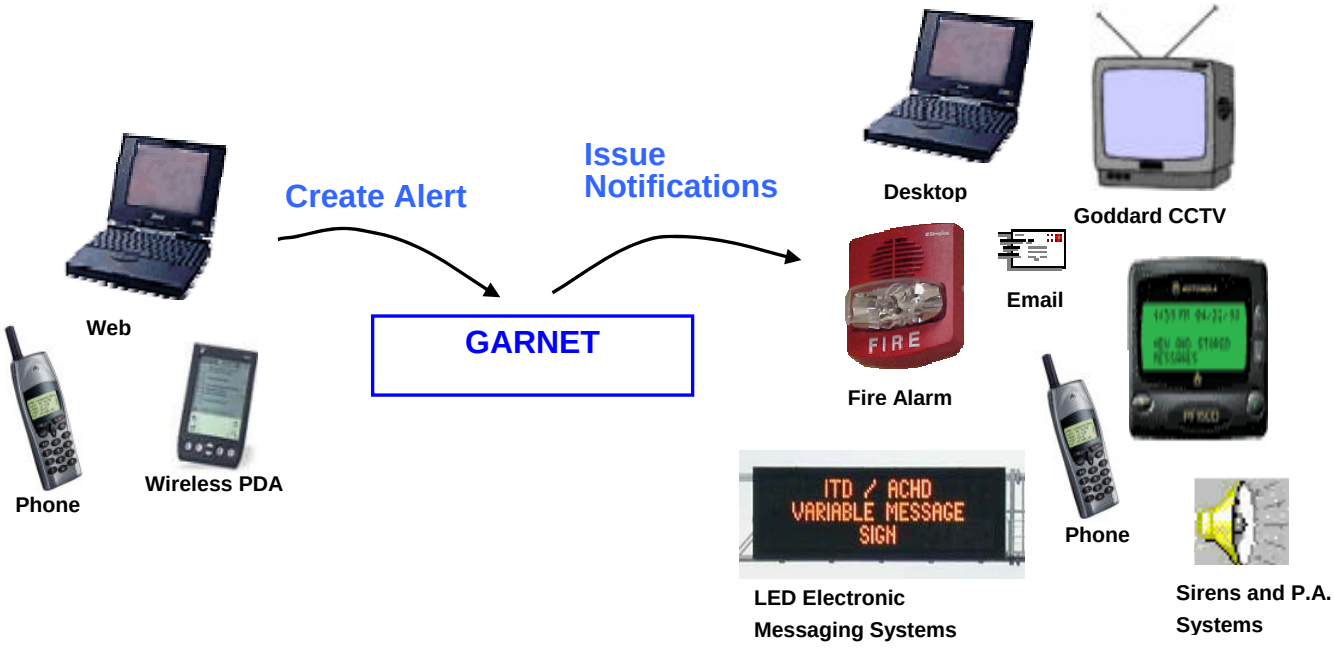
The current project scope encompasses the functionality of GARNET for the initial rollout to GSFC's Greenbelt facility. This document outlines high-level requirements that are considered core and generic to the GARNET system. Additionally, the document specifies requirements for GARNET 2.0. In the case that a customer wishes to alter and/or extend GARNET 2.0, an additional requirements document should be produced outlining the altered and/or new functionality.

1.5 References

The GARNET Operational Concept Document (OCD) outlines how the GARNET system will operate. The document describes high-level user interactions and system behaviors.

2 Overall Description

2.1 Product Features



The figure above provides a high-level vision of the GARNET system. The vision includes the idea of having multiple mechanisms available to create and activate alert notifications. Some sample creation mechanisms include computers with network access, phones, and even wireless devices such as a Personal Digital Assistants (PDAs).

Once an authorized person creates an alert, the GARNET system is responsible for determining whom to notify and how to contact the affected people. There are numerous potential notification mediums that could be integrated, including computer desktops, E-mail messages, pagers, and phones. The personal computer provides an excellent way to contact people quickly. One of the key benefits of notifying people via their desktops is the ability to require a person to acknowledge the alert. When a critical alert is received, a window will pop up in front of all the other windows on the user's desktop, requiring a user to minimize or close the window in order to continue working.

The GARNET infrastructure will be utilize the strengths of existing alert systems, augmented by desktop computer alerts. By using multiple alerting mechanisms, GARNET can contact people, including the hearing- and sight-impaired, at their computers, as well as within meeting rooms, bathrooms, and halls.

An IT-based alerting system provides these benefits:

- Makes use of infrastructures and systems already in place (e.g. computer networks, desktop computers).
- Provides multiple ways to create an alert and multiple mediums to distribute an alert. No dependency on a single alert mechanism.
- Contacts more people, including the disabled, more quickly by using multiple alert mediums.
- Targets alerts based on criteria such as a specific building, geography, alert type, and alert severity.
- Provides fine-grained control to notify only those people affected by the alert as determined by subscriber profiles.
- Includes details regarding the nature of the alert, and recommended actions/instructions.
- Requires a small amount of resources to perform tasks such as backups, system upgrades, security audits, etc.

2.2 User Classes and Characteristics

The system shall provide multiple system privileges. Each user in the system can be granted privileges. Note, a user may belong to multiple user classes, and therefore, will be granted multiple sets of privileges. For example, a user may be granted alert creation privileges in addition to being able to subscribe to alerts. Additionally, for a smaller deployment of a GARNET system a single user may take on both system administrative duties, such as system upgrades and security audits, in addition to administrative tasks, such as user account management. GARNET will support the following types of user privileges:

- System Administrator

  A user who had been granted system administrator privileges shall be able to gain access to the server machine(s) to perform maintenance, upgrades, security audits, GARNET desktop client installations, etc.

- Administrator

  A user who has been granted administrative privileges shall be able to create/edit/remove user accounts, create/edit/remove subscription groups, grant user privileges, and create/edit/remove alert categories and severities.

- Alert Creator

  A user who has been granted alert creation privileges shall be able to create alerts for a specific alert category and severity. A user may be granted privileges to create alerts for multiple category/severity pairs.

- Alert Subscriber

  A user who has alert subscriber privileges can subscribe to receive alerts for alert categories/severities for which s/he has been granted access. S/he may also search for historical alerts by categories/severities for which s/he has been granted access.

3 System Functional Requirements

This section of the document outlines the functional requirements broken down by functional area.

3.1 Alert Definition

3.1.1 High-Level

ID	Requirement	Justification
REQ-0101000	An alert contains information explaining the details of alert including information to target the alert to affected people and the priority/severity level of the alert.	High-level description of an alert. Key points include details about the alert. Ability to target the alert to affected people. Priority level of an alert.

3.1.2 GARNET 2.0

ID	Requirement	Justification
REQ-0101000	An alert contains a title.	Brief title for the alert that relays the main idea/reason for the alert.
REQ-0101010	An alert contains a description.	An alert description is critical information that should be available to alert recipients.
REQ-0101020	An alert contains an optional URL to extra info and/or details pertaining to the alert.	For example, if a weather alert is being issued, the creator may also provide a link to weather.com
REQ-0101030	An alert contains a creation timestamp.	A timestamp represents when an alert was received by the system to be sent to affected parties.
REQ-0101040	An alert contains a creator.	Identification criteria which specifies who created and submitted the alert to the system.

ID	Requirement	Justification
REQ-0101050	An alert contains at least one associated category.	An alert category provides the information necessary to determine who should be notified.
REQ-0101060	An alert contains a severity.	An alert severity is critical information that should be available to alert recipients to express the level of importance of the alert. The designation of an alert severity provides information necessary to determine who should be notified.
REQ-0101070	An alert category has a name.	A short descriptive name for the category that will be used to classify alerts.
REQ-0101071	An alert category has a short name.	The short name is used to classify alerts for SMS devices.
REQ-0101080	An alert category has a description.	Outlines what the category includes and when/how it should be used. Example categories include weather, IT, Code 588, Security and Safety, etc.
REQ-0101090	An alert category has a point of contact including a name, phone, E-mail.	This person is the 'keeper' of the category.
REQ-0101100	An alert category has a creation time.	When the category was created.
REQ-0101110	An alert severity has a name.	A short descriptive name for the severity that will be used to classify alerts.
REQ-0101111	An alert severity has a short name.	The short name is used to classify alerts for SMS devices.
REQ-0101120	An alert severity has a description.	Outlines what the severity means and when/how it should be used. Example severities include, Informational, Warning, Critical/Life-threatening. This description should provide a clear description such that the severity ordering is obvious to the user.
REQ-0101130	An alert severity has a unique priority order. The highest priority shall be 1.	This forces an ordering to the different severities. Critical is higher priority than informational. Level of importance.
REQ-0101150	The system shall have a CRITICAL/LIFE-THREATENING severity priority 1.	

ID	Requirement	Justification
REQ-0101160	Reserved.	
REQ-0101170	Reserved.	
REQ-0101180	The system shall have an INFORMATIONAL severity with priority 4.	

3.2 Login

Login is one way in which the system takes security measures to control access to privileged system functions. Login functionality is a high system priority. A user must log in to the system to gain access to perform a privileged system function such as alert creation, user profile changes, etc. Upon successful login the system will allow the user to perform system functions for which s/he has privileges. If a user is unable to successfully login the system will not allow the user to perform any system functions that require privileges.

3.2.1 High-Level

ID	Requirement	Justification
REQ-0102000	The system shall require a user to successfully log in to the system and have appropriate privileges to perform alert creation, view/edit profile, and/or search for historical alerts.	Expresses at a high level that a user needs to log in to perform any system functions that require privilege. Also outlines at a high level what those functions include.
REQ-0102010	The system shall not grant access to a privileged system function to a user who has failed to be authenticated to perform the function.	Expresses a need for the system to provide a method for user authentication and system control over access to privileged functions.

3.2.2 GARNET 2.0

ID	Requirement	Justification
REQ-0102020	A user shall supply a username and password to attempt logging in to the system.	Explains what a user needs to provide to logon to the system.
REQ-0102040	A user may have his/her password reset to a random password and E-mailed to him/her by using his/her username and answering his/her secret question correctly.	Handles the case when a user forgets his/her password.

ID	Requirement	Justification
REQ-0102050	The system shall not grant access to a privileged system function to a user who has failed login five consecutive times using the same username five consecutive times.	Security – NPG2810.1

3.3 User Profile Management

A user profile contains information to outline what type of alerts a user wishes to receive and through what media s/he would like to receive them. User profiles are a critical piece of the application because they allow the system to determine whom to notify with an alert. The following set of requirements outline the capabilities the system will provide to a user to manager his/her profile.

3.3.1 High-Level

ID	Requirement	Justification
REQ-0103000	A user shall be required to have a user profile.	Necessary, otherwise a user would not be able to receive any alerts.
REQ-0103010	A user shall be required to log in to access his/her user profile information.	
REQ-0103020	A user profile contains alert subscriptions describing the type of alerts a user is interested in being notified about and the mediums through which the user would like to be notified.	High-level explanation of what is included in a user profile.
REQ-0103030	A user profile contains login credentials.	
REQ-0103040	A user may only edit the information in his/her profile that he/she is permitted to change.	

3.3.2 GARNET 2.0

ID	Requirement	Justification
REQ-0103060	A user profile contains notification rules. A notification rule contains a category, severity, and one or more notification mediums.	Outlines the categories of alerts a user wants to receive. The system will use this info to determine if an alert is relevant to a user.

ID	Requirement	Justification
REQ-0103070	A user profile contains notification medium configurations.	A notification medium is a tool that can be used by the GARNET system to a contact a user with alert details. A notification medium configuration supplies the information necessary to a specific medium in order for GARNET to be able to contact the user.
REQ-0103080	An E-mail notification medium configuration requires an E-mail address.	Information required for a user to receive alerts via E-mail.
REQ-0103090	A user profile may optionally include multiple E-mail configurations.	A user may wish to receive alerts at multiple E-mail accounts.
REQ-0103091	An E-mail notification medium configuration allows a user to select whether the medium is an SMS device.	Many alphanumeric pagers and cell phones use Small Message System (SMS) protocol, which restricts the size of the message received.
REQ-0103100	Reserved.	
REQ-0103110	Reserved.	
REQ-0103120	A user profile shall contain a notification priority that determines the order in which users are notified.	Some users may need to be notified prior to other users. For example, a building FOM should be notified of emergencies before other building occupants and therefore will receive a high priority.
REQ-0103130	The system shall provide a notification priority NORMAL.	Default out-of-the box system provides a notification priority NORMAL.
REQ-0103140	The system shall provide a notification priority HIGH.	Default out-of-the box system provides a notification priority NORMAL.
REQ-0103160	A user shall be able to add/edit/remove/view notification rules that he/she has privilege to change in his/her user profile.	Some rules in a user profile may be setup by an administrator and will not be able to be modified by anyone other than an administrator. Addressed in the administrative requirements.
REQ-0103170	A user shall be able to view the categories and associated severities and notification mediums that are required in his/her user profile. The user will not be able to remove these rules.	In the case that some users should not have an option to be subscribed to certain severities and categories.
REQ-0103180	A user may optionally add additional notification mediums to the required notification rules contained in his/her user profile.	
REQ-0103181	A user shall have the ability to send a test message to the notification mediums added to the user's profile.	Reduces the need for tech support.

ID	Requirement	Justification
REQ-0103190	A user shall be able to add/edit/remove/view E-mail notification mediums from his/her user profile.	
REQ-0103200	Reserved.	
REQ-0103210	A user profile shall contain user credentials including a first name, last name, middle initial, password, secret question, secret answer, and E-mail address.	
REQ-0103211	A user profile shall contain user information including organization code, mail code, facility, building, room, phone number	This user information allows notification rules to be set based on the person's building, organization code, mail code, etc.
REQ-0103220	A user shall be able to change his/her password contained in his/her user credentials.	
REQ-0103230	A user shall be able to set/edit his/her secret question and secret answer in his/her user credentials.	
REQ-0103240	Reserved.	
REQ-0103250	Reserved.	

3.4 Alert Creation

Alert creation is a critical system function that particular users are granted privilege to perform. The following outlines the requirements surrounding alert creation.

3.4.1 High-Level

ID	Requirement	Justification
REQ-0104000	An authorized user shall be able to create an alert and target the alert criteria including alert category and severity.	High-level description of how a user creates an alert.
REQ-0104010	The system shall store details about each alert created.	We need a history of the alert created in the system for multiple reasons. First for security purposes so that misuse of the system can be tracked, and secondly so that users can search for historical alerts.

3.4.2 GARNET 2.0

ID	Requirement	Justification
REQ-0104020	Alert creation shall be accessible via a supported web browser over a secure socket.	For the initial production release, GARNET will provide a web front-end for alert creation.
REQ-0104030	The user must successfully log in to the system and have the appropriate privileges to access alert creation.	Only authorized users are allowed to create alerts.
REQ-0104040	The user must supply an alert title.	Some mediums the alert is issued to may only include the title rather than the full alert description. Title should be short and relay the main idea of the alert in a short concise manner.
REQ-0104050	The user must supply an alert description.	An alert description is critical information that should be available to alert recipients. Should include the complete details/instructions related to the alert.
REQ-0104060	The user may optionally supply a URL that contains information relevant to the alert.	Points the user to additional information pertaining to the alert. For example, weather.com.
REQ-0104070	The user must supply a single alert severity.	An alert severity is critical information that should be available to alert recipients. The designation of an alert severity provides information necessary to determine who should be notified and also relays the level of importance to the user. Each alert will only have a single severity.
REQ-0104080	The user must supply one or more alert categories.	An alert category provides the information necessary to determine who should be notified. Each alert with have one or more associated categories.
REQ-0104090	The user shall only be able to create an alert for categories/severities that he/she has privileges for.	Some users will have privilege to create an alert for a particular category and severity level.
REQ-0104100	The user must review an alert prior to submitting it.	An attempt to reduce errors during alert creation.
REQ-0104110	The system shall store the alert timestamp, creator, title, description, URL, category(s), and severity.	The specifics of what the system needs to store associated with the alert for security reasons and searches.

3.5 Alert Notifications

This section of requirements outlines details pertaining to capabilities the system provides associated with alert notifications. A key goal of the system is to provide fine-grained notification control so that only users affected by or interested in the alert with receive the alert. Additionally, another goal of the system includes sending detailed information with the alert.

3.5.1 High-Level

ID	Requirement	Justification
REQ-0105000	The system shall provide fine-grained alert notification control to only notify those users affected by the alert by matching the alert criteria with user profiles.	Users only subscribe to categories they are interested in. Besides general, site-wide alerts, this prevents users from being inundated with inconsequential notifications.
REQ-0105010	The system shall issue detailed alert information, including alert description and severity to mediums where it is feasible.	It is possible for e-mail notifications to contain elaborate detailed information since it can be represented by text. However, there is no means for fire alarms to represent information with such fidelity; they simply ring and strobe. We are limited by the capabilities of the alert medium.
REQ-0105020	The system shall support notifying users via GARNET computer desktop client, E-mail, and SMS devices.	At a minimum the system must support these media to contact users.
REQ-0105030	The system shall provide a way to prioritize the order in which users are issued notifications.	Some users should be notified of an alert prior to other users. For example, FOMs should be notified of an alert first.

3.5.2 GARNET 2.0

ID	Requirement	Justification
REQ-0105040	The system shall support issuing an alert notification via E-mail.	E-mail provides a quick easy way to notify affected parties of an alert.
REQ-0105050	The system shall support issuing an alert notification to an SMS device such as alphanumeric pager or cell phone via an E-mail interface.	Text messaging provides a easy way to notify affected parties of an alert.
REQ-0105060	The system shall support issuing an alert notification to a GARNET computer desktop client.	A desktop computer that is connected to a network provides a quick easy way to notify people of an alert. It also provides a means for the client to have to recognize the alert.
REQ-0105070	The system shall issue a notification to an affected party within 5 minutes from when the alert was created.	A key point to the system is quick notification. The system needs to be able to send out alert notifications as quickly as possible.
REQ-0105080	The system shall support notifying users via a GARNET desktop client. GARNET desktop client must have outgoing internet access on at least one undedicated TCP/UDP port.	Required by many firewall implementations.

ID	Requirement	Justification
REQ-0105090	The system shall determine notification recipients based on user notification rules contained within user profiles. Specifically, the alert category and severity must match the category and severity of a rule contained in the user's profile in order for the user to be issued a notification(s).	Matching alert characteristics to user profiles provides the mechanism to only contact the affected people or those whom would be interested in the alert.
REQ-0105100	The system shall issue notifications based on the notification priority contained in each user profiler. A user with notification priority HIGH will be issued notifications prior to a user with a notification priority of NORMAL.	FOMs and other emergency response personnel should be notified of an alert before all others.
REQ-0105110	The system shall determine the notification mediums to issue notifications to, based on the notification media associated with the matching notification rule.	Us the user notification rules to determine which medium(s) to issue the alert to.
REQ-0105120	A user shall not receive duplicate alerts on the same notification medium.	In the case that an alert is associated with multiple categories and a single client/user matches multiple times - only one notification will be issued to each relevant alert notification medium.
REQ-0105130	An alert issued via E-mail will contain the alert title, description, URL if provided, timestamp, severity, and category(s). A URL to the GARNET system to retrieve the full details about the alert will also be included.	Details what information is included in an E-mail notification.
REQ-0105140	An alert issued to an SMS device will contain the alert title, timestamp, severity, and category(s). Some amount of the description will be included, up to the SMS limit.	Details what information is included in an SMS device notification.
REQ-0105141	The total number of characters for an alert sent to an SMS device will not exceed 140 characters, including the e-mail headers.	SMS devices are restricted to as little as 140 characters per message.

ID	Requirement	Justification
REQ-0105150	An alert issued to a GARNET desktop client will contain the alert title, URL if provided, timestamp, severity, and category(s). Some TBD amount of the description will be included. A URL to the GARNET system to retrieve the full details about the alert will also be included.	Details what information is included in a GARNET client desktop notification.
REQ-0105160	An alert notification issued to a GARNET desktop client will be sent over a secure communication medium.	For security purposes alert notification will be encrypted whenever possible during transmission. Not feasible via E-mail and alphanumeric pager notifications.

3.6 Alert Searches

Alert searches provide the ability for a user to get the details about a historical alert. For example, if an alert about road closings is issued, a user may need to refer back to the alert for the specific dates. Additionally, alert searches will be needed for security reasons to track any misuse of the system.

3.6.1 High-Level

ID	Requirement	Justification
REQ-0106000	A user must successfully log in to the system to access alert search functionality.	Alert search is a privileged system function.
REQ-0106010	The user shall be able to search through historical alerts that s/he has privilege to view.	Initially, users will have privilege to view any historical alert regardless of whether they received the original alert.
REQ-0106020	The system shall provide a means for a user to search alerts that have not been archived.	Once an alert is archived it is not longer available to be searched through the normal means.

3.6.2 GARNET 2.0

ID	Requirement	Justification
REQ-0106030	Reserved	Initially, users will have privilege to view any historical alert regardless of whether they received the original alert..
REQ-0106040	A user shall be able to search for previously issued alerts based on a data/time range, category, severity, and title.	

3.7 GARNET Desktop Client

The GARNET desktop client will be notification medium that runs on users desktop computers. It will receive alerts from the GARNET system and make then available directly as a users desktop computer.

3.7.1 High-Level

ID	Requirement	Justification
REQ-0107000	A user shall be able to manually start the GARNET desktop client on their desktop machine.	
REQ-0107005	The GARNET desktop client shall be able to be configured to start automatically upon desktop startup/boot.	
REQ-0107010	A user shall be able to specify their GARNET user login criteria to the client.	When starting the desktop client the user can enter their GARNET username and password so that the desktop client can receive alerts for the specified user.
REQ-0107020	The GARNET computer desktop client shall require a user to acknowledge a critical alert that it received prior to resuming work on his/her computer.	
REQ-0107030	Alerts received via the GARNET desktop client that require acknowledgement, shall not alter/affect actively running programs and shall allow users to return to previous work after acknowledgement.	We need to make it clear that GARNET will not conflict with other running applications. The other applications data will not be altered in any way when an alert is received.

3.7.2 GARNET 2.0

ID	Requirement	Justification
REQ-0107040	The system shall provide for password synchronization between the GARNET Server and the desktop client.	The user should not have to change his/her password in two places.
REQ-0107050	The system shall provide an automatic update capability to ease delivery of enhancements to the desktop client.	

3.8 Administrative

GARNET has several administrative functions that are necessary to manage users in addition to controlling how an alert can be targeted to interested users only.

3.8.1 High-Level

ID	Description	Justification
REQ-0108000	An authorized administrator shall be able to create/edit/remove user accounts and profiles.	
REQ-0108010	An authorized administrator shall be able to create/edit/remove user alert subscriptions. A user shall not be able to alter an administrator specified alert subscription.	
REQ-0108020	An authorized user may grant privileges to a user.	

3.8.2 GARNET 2.0

ID	Description	Justification
REQ-0108030	An authorized administrator may create a user account with the following data: First name, Last Name, E-mail address	Details what is necessary to create a user account.
REQ-0108040	An authorized administrator may mark a user account as inactive.	We don't want to permanently delete user accounts but rather mark them as inactive for security purposes and historical alert tracking.
REQ-0108045	An authorized administrator may activate a user account that was disabled/inactive.	
REQ-0108050	An authorized administrator may edit a user profile by modifying the following data: first name, last name, middle initial, e-mail address, organization code, mail code, facility, building, room, required notification rules, notification medium configurations, and notification priority.	
REQ-0108060	An authorized administrator may create/edit/remove alert categories.	
REQ-0108070	An authorized administrator may reset a password for any user.	

ID	Description	Justification
REQ-0108071	The system will warn the administrator if an e-mail informing the user of a reset password could not be sent successfully.	
REQ-0108080	An authorized administrator shall be able to grant and revoke administrative and alert creation per categories/severities privileges to any user.	
REQ-0108090	An authorized administrator may create/edit/remove a subscription group. A subscription group has a name, description, and one or more related alert categories.	Used to make it easy for an administrator to create a user account and assign the alert categories they have privilege to. Instead of assigning each individual category, the administrator will be able to assign by specific category and also assign a user to a subscription group(s).
REQ-0108100	An authorized administrator may assign a user to a subscription group(s) and the user will then have privilege to subscribe to all alert categories associated with the subscription group.	We need to decide if we are going to do this. May be useful to have for FOMs, Directors of, etc.
REQ-0108110	The system shall store a maximum of ten million alerts. If there are more than ten million alerts stored a portion of the alerts shall be archived, starting with the oldest ones first.	
REQ-0108120	A system administrator shall be able to configure how old an alert must be in order for it to be archived.	
REQ-0108140	The System shall allow the addition of users from the x.500 directory.	
REQ-0108150	The system shall include the last name, first name, middle initial, e-mail address, building, organizational code, mail code, and uniqueID from the x.500 directory.	
REQ-0108160	The system shall update the last name, first name, middle initial, e-mail address, building, organizational code, and mail code based on the uniqueID, as changes are made to the x.500 directory.	
REQ-0108170	The system shall assign users to required building groups based on their building assigned in the x.500 directory.	

ID	Description	Justification
REQ-0108180	The system shall update building and code lists based on x.500 updates.	
REQ-0108190	The administrator shall be able to add users from the x.500 directory based on the users' code, building, or name.	
REQ-0108200	The system shall delete users that are no longer found in the x.500 directory.	
REQ-0108210	The system shall create and update categories based on buildings found in x.500.	

3.9 Documentation and Help

3.9.1 High-Level

ID	Description	Justification
REQ-0109000	The system shall provide on-line help.	While a user is using the system they shall be able to access help documentation via a system function.
REQ-0109010	The system shall provide a complete user manual.	How to login. How to manage your profile. How to create an alert. Etc.
REQ-0109020	There shall be a GARNET desktop client user manual containing instructions for each platform.	
REQ-0109030	The system shall have a security plan.	Outlines the technical defenses the system has to provide security in addition to procedures associated with keeping the system secure and audit plans.
REQ-0109040	The system shall have a system administrators guide.	Outlines things such as how to perform upgrades, installation, deployment, etc.
REQ-0109050	The system shall have a system architecture and design guide.	For ongoing maintenance and add-on functionality. Explains how the system is extensible and how best to add new ways to create alerts and new notification medium support.
REQ-0109060	The system shall have an Administrators user manual.	How to create/edit/remove user account. How to grant privileges. How to manage subscription groups including alert categories. How to reset user passwords.

3.10 Logging

The following list of requirements describes the necessary capabilities of the logging system. Logs are invaluable for assessing security effectiveness, assessing system health, and documenting user and system activities.

3.10.1 High-Level

ID	Description	Justification
REQ-0110000	Faults in the operation of the system shall be logged at the time they were detected	All fault must be accounted for
REQ-0110010	All system logs shall be tamper-resistant	We need to make sure we maintain log integrity

3.10.2 GARNET 2.0

ID	Description	Justification
REQ-0110020	Log entries shall contain a timestamp, a description, and a severity level such as error, warning, info, etc. Events occurring as a result of user actions shall also contain the user's identifier.	This is a list of minimal critical information for tracing
REQ-0110030	Any alteration of data through administrative functions shall be logged.	We should log changes to user profiles, groups, categories, severities to create an audit trail
REQ-0110040	All failed login attempts shall be logged.	Required for security incident detection and response.
REQ-0110050	All alerts created shall be logged.	We need to keep an record of alerts
REQ-0110060	Only authorized administrators/operators shall have the ability to view logs.	No other users need to view the logs. It keeps users from misusing the logs through espionage
REQ-0110070	All logs shall be archived weekly.	This will save space on the primary storage device.
REQ-0110080	If the log capacity has been reduced to 20% free space, the system shall send an alert to a system administrator indicating the logs need maintenance.	We may need to occasionally rotate the logs when they overflow due to large bursts in activity. If the logs continually overflow, the log capacity should be increased.

4 System Nonfunctional Requirements

4.1 Performance Requirements

The following is a list of minimal performance requirements of the prototype GARNET 2.0 system. The purpose of specifying these requirements is to establish a baseline performance needed for an effective implementation of GARNET.

4.1.1 GARNET 2.0

ID	Description	Justification
REQ-0201000	The GARNET system shall not be inoperable more than 8 hours per year	Provide some time for maintenance. This requirement may be difficult to prove we satisfy this.
REQ-0201010	The GARNET system shall accommodate up to 10,000 users.	The upper bound is based on predicted storage capacity
REQ-0201020	The GARNET system shall accommodate up to 40,000 notification clients regardless of medium.	The upper bound is based on predicted storage capacity
REQ-0201030	The GARNET system shall be capable of transmitting 50 alerts simultaneously.	This upper bound is based on predicted computing capacity.

4.2 Security Requirements

This section details security functions and characteristics needed to maintain system integrity, confidentiality, and availability. Many requirements listed here are derived from NPG 28010.1.

4.2.1 High-Level

ID	Description	Justification
REQ-0202000	Network access to the alert creation server shall be restricted to unauthorized machines.	NPG2810.1 Section A.7.1
REQ-0202010	System shall ensure that passwords are stored confidentially.	NPG2810.1 Section A.6.3.7
REQ-0202020	The system shall ensure the confidentiality and integrity of communication between the system and remote clients.	NPG2810.1 Section A.7.4.3
REQ-0202030	Security logs shall record security-relevant events.	NPG2810.1 Section A.6.1.3
REQ-0202040	Critical system data modifications shall be recorded.	NPG2810.1 Section A.6.1.3

ID	Description	Justification
REQ-0202050	The system shall prevent unauthorized users from accessing the system.	High level authentication requirement
REQ-0202060	The system shall implement controls to ensure the privacy of information and individuals are not compromised.	High level requirement for confidentiality
REQ-0202070	The system shall implement controls to ensure that the authenticity of data is preserved.	High level requirement for integrity

4.2.2 GARNET 2.0

ID	Description	Justification
REQ-0202100	User secret answers shall be stored confidentially.	NPG2810.1 Section A.6.3.7
REQ-0202110	The system shall deter one or more users from successfully using a denial of service attack by flooding the system with new alert requests.	Prevent DoS attacks
REQ-0202120	After five consecutive failed login attempts, a user account shall be disabled. Only a privileged administrator may reactivate a user account.	NPG2810.1 Section A.6.4.2
REQ-0202130	The system shall use the Data Encryption Standard (DES) to secure communications between the system and remote clients	NGP2810.1 Section A.6.9
REQ-0202140	The system shall ensure users do not choose trivial passwords as defined in NPG2810.1 Section A.6.3.3	NPG2810.1 Section A.6.3.3
REQ-0202150	The system shall not display users' password when typed	NPG2810.1 Section A.6.3.8
REQ-0202160	Password changes shall be logged. User ID and date/time of changes made shall be recorded	NPG2810.1 Section A.6.3.8
REQ-0202170	The system shall ensure a user changes his/her password after the first login after a password reset.	NPG2810.1 Section A.6.3.9
REQ-0202180	The system shall ensure users read and agree to usage terms specified in a warning banner upon logon	NPG2810.1 Section 4.10

ID	Description	Justification
REQ-0202190	Successful and failed logons/logoffs shall be recorded	NPG2810.1 Section A.6.1.3
REQ-0202200	The system shall ensure that only authorized personnel shall shutdown the system.	NPG2810.1 Section A.6.1.5
REQ-0202210	The system shall remind users to change passwords at least every 90 days	NPG2810.1 Section A.6.2.4
REQ-0202220	The system shall ensure that user accounts are suspended if passwords are not changed at least every 120 days	NPG2810.1 Section A.6.2.4
REQ-0202230	User passwords shall be a minimum of eight characters containing at least one character each from at least three of the following sets: uppercase letters, lowercase letters, numbers, and special characters.	NPG2810.1 Section A.6.3.2

4.3 Fault Tolerance

This section describes required system features to detect faults in an operational system and features necessary to maintain system availability in the event of the occurrence of such faults.

4.3.1 GARNET 2.0

ID	Description	Justification
REQ-0203010	Faults in issuing alert notifications shall be detected within 1 minute	A minimum detection time must be established
REQ-0203020	Faults in alert creation shall be detected within 1 minute	A minimum detection time must be established
REQ-0203030	Hardware system failures shall be detected within 1 minute	A minimum detection time must be established
REQ-0203040	Recovery from single hardware system failures shall take less than 30 seconds	A minimum recovery time must be established
REQ-0203050	Recovery from any single point of failure shall take less than 15 minutes	A minimum recovery time must be established

4.4 Software Quality Attributes

4.4.1 High-Level

ID	Description	Justification
REQ-0204000	The system architecture shall be extensible to be able to support multiple methods to create an alert.	The overall architecture should be designed such that it will be able to be extended to support multiple mechanisms to create an alert. For example via http, phone, etc.
REQ-0204010	The system architecture shall be extensible to be able to issue notifications to multiple mediums.	Notify via GARNET desktop client, E-mail, pager, CCTV, phone, fire alarm, and other futuristic mediums.
REQ-0204020	The system architecture shall be designed to be scaleable and reliable.	The number of users can grow and the system will be able to scale to handle them if we add more machines to handle them. The system shall be available when necessary and must provide a fail-over mechanism.
REQ-0204030	The system shall support end-users with disabilities according to Section 508 of the Rehabilitation Act.	Need to support users with disabilities.
REQ-0204040	The GARNET computer desktop client shall run on multiple platforms.	
REQ-0204050	The system shall provide failover capabilities to ensure reliability.	
REQ-0204060	The GARNET desktop client shall support end-users with disabilities according to the final version of the draft Notice of Proposed Rulemaking on Standards for Electronic and Information Technology implementing Section 508 of the Rehabilitation Act.	

5 Other Requirements

5.1 System Constraints

This section lists constraints set upon the implementation of GARNET 2.0. The intent of system constraints is to establish known limitations on operation system characteristics.

5.1.1 GARNET 2.0

ID	Description	Justification
CON-0101040	The GARNET system client applications shall be supported on the following platforms: PC Windows 2000 SP3 and XP SP2; Red Hat 8.0; Mac OSX 10.2.x	This specifies minimum operating systems needed to implement GARNET 2.0
CON-0101030	The GARNET system user interface shall be supported by the following platforms and web browsers: PC Windows 2000 SP3 and XP SP2 -- IE 6.x and Netscape 7.0; Red Hat 8.0 -- Netscape 7.0; Mac OSX 10.2.x -- IE 5.2	This specifies minimum browsers needed to implement GARNET 2.0
CON-0101050	The minimum hardware requirements of the GARNET client software for PC-based clients are: CPU -- Intel Pentium 4; 512MB RAM; 80GB Harddisk; CDRom drive;	This specifies minimum hardware needed to implement a GARNET 2.0 desktop client on a PC.
CON-0101051	The minimum hardware requirements of the GARNET client software for MAC-based clients are: CPU____; 512MB RAM; 80GB Harddisk; CDRom drive;	This specifies minimum hardware needed to implement a GARNET 2.0 desktop client on a Mac.
CON-0101052	The minimum hardware requirements of the GARNET client software for Unix-based clients are: CPU -- Intel Pentium 4; 512MB RAM; 80GB Harddisk; CDRom drive;	This specifies minimum hardware needed to implement a GARNET 2.0 desktop client on a Unix machine.